What is claimed is:

1. A method for generating and verifying an ID-based blind signature by using bilinear parings, the method comprising the steps of:

generating system parameters, selecting a master key, and then disclosing the system parameters by a trust authority;

generating a private key by using a signer's identity and the master key, and then transferring the private key to the signer through a secure channel by the trust authority;

receiving and storing the system parameters by a user and receiving and storing the system parameters and the private key by the signer;

computing a commitment by using at least one of the system parameters, and then sending the commitment to the user by the signer;

blinding a message by using the commitment and a public key based on the signer's identity, and then sending the blinded message to the signer by the user;

signing the blinded message by using the private key, and then sending the signed message to the user by the signer;

unblinding the signed message by the user; and

verifying the signature by the user,

wherein the system parameters include G_1, G_2, e, q, P,

P_{pub}, H_1 and H_2, where G_1 is a cyclic additive group whose order is a prime q, G_2 is a cyclic multiplicative group of the same order q, e is a bilinear paring defined by $e: G_1 \times G_1 \rightarrow G_2$, P is a generator of G_1, P_{pub} is the trust authority's public key described by $P_{pub} = s \cdot P$, where s is the master key, and H_1 and H_2 are hash functions, respectively, described by $H_1: \{0,1\}^* \rightarrow Z_q^*$ and $H_2: \{0,1\}^* \rightarrow G_1$, where Z_q^* is a cyclic multiplicative group,

wherein the public key Q_{ID} is described by $Q_{ID} = H_2(ID)$, where ID is the signer's identity, and the private key S_{ID} is described by $S_{ID} = s \cdot Q_{ID}$, and

wherein the commitment U is described by $U = r \cdot Q_{ID}$, where r is a random number the signer chooses.

2. The method of claim 1, wherein the blinded message h is described by $h = \alpha^{-1} H_1(m, U') + \beta$, where m is a message to be sent, U' is described by $U' = \alpha U + \alpha\beta Q_{ID}$ and α and β are blinding factors belonging to Z_q^*.

3. The method of claim 2, wherein the signed message is described by $V = (r + h) S_{ID}$.

4. The method of claim 3, wherein the step of unblinding is performed by using formula $V' = \alpha V$.

5. The method of claim 4, wherein the step of verifying

is preformed by using following equations:

$$e(V', P)$$

$$= e(U', + H_1(m, U')Q_{ID}, P_{pub}).$$

6. An apparatus for generating and verifying an ID-based blind signature by using bilinear parings, the apparatus comprising:

means for generating system parameters, selecting a master key, and then disclosing the system parameters by a trust authority;

means for generating a private key by using a signer's identity and the master key, and then transferring the private key to the signer through a secure channel by the trust authority;

means for receiving and storing the system parameters by a user and receiving and storing the system parameters and the private key by the signer;

means for computing a commitment by using at least one of the system parameters, and then sending the commitment to the user by the signer;

means for blinding a message by using the commitment and a public key based on the signer's identity, and then sending the blinded message to the signer by the user;

means for signing the blinded message by using the private key, and then sending the signed message to the user by the signer;

means for unblinding the signed message by the user; and

means for verifying the signature by the user,

wherein the system parameters include G_1, G_2, e, q, P, P_{pub}, H_1 and H_2, where G_1 is a cyclic additive group whose order is a prime q, G_2 is a cyclic multiplicative group of the same order q, e is a bilinear paring defined by $e: G_1 \times G_1 \rightarrow G_2$, P is a generator of G_1, P_{pub} is the trust authority's public key described by $P_{pub} = s \cdot P$, where s is the master key, and H_1 and H_2 are hash functions, respectively, described by $H_1: \{0,1\}^* \rightarrow Z_q^*$ and $H_2: \{0,1\}^* \rightarrow G_1$, where Z_q^* is a cyclic multiplicative group,

wherein the public key Q_{ID} is described by $Q_{ID} = H_2(ID)$, where ID is the signer's identity, and the private key S_{ID} is described by $S_{ID} = s \cdot Q_{ID}$, and

wherein the commitment U is described by $U = r \cdot Q_{ID}$, where r is a random number the signer chooses.

7. The apparatus of claim 6, wherein the blinded message h is described by $h = \alpha^{-1} H_1(m, U') + \beta$, where m is a message to be sent, U' is described by $U' = \alpha U + \alpha\beta Q_{ID}$ and α and β are blinding factors belonging to Z_q^*.

8. The apparatus of claim 7, wherein the signed message is described by $V = (r + h) S_{ID}$.

9. The apparatus of claim 8, wherein the means for unblinding is performed by using formula $V' = \alpha V$.

10. The apparatus of claim 9, wherein the means for verifying is preformed by using following equations:

$$e(V', P) = e(U', + H_1(m, U')Q_{ID}, P_{pub}).$$